Tuomas Hakkarainen

On the computation of class numbers of real abelian fields

Turku Centre *for* Computer Science

TUCS Technical Report
No 770, May 2006

On the computation of class numbers of real abelian fields

Tuomas Hakkarainen
Department of Mathematics & TUCS - Turku Centre for Computer Science
University of Turku
FI-20014 Turku
Finland
tuheha@utu.fi

TUCS Technical Report
No 770, May 2006

Abstract

In this paper we give a procedure to search for prime divisors of class numbers of real abelian fields and present a table of odd primes < 10000 not dividing the degree that divide the class numbers of fields of conductor ≤ 2000. Cohen–Lenstra heuristics allow us to conjecture that no larger prime divisors should exist. Previous computations have been largely limited to prime power conductors.

Keywords: Class numbers, computation, abelian fields, units

TUCS Laboratory
Discrete Mathematics for Information Technology

1 Introduction

Class numbers of real abelian fields are at least by present-day knowledge very hard to compute in practice. This is because they are so closely related to the fundamental units, which are difficult to compute or even estimate. Rough estimates that exist in turn lead to poor upper bounds for class numbers. Only for fields of small conductors one can bound class numbers decently with Odlyzko's tables of discriminant bounds; using them F. van der Linden [14] was able to determine (assuming GRH in some cases) the class numbers of all the real abelian fields of conductor ≤ 163. On the other hand R. Schoof [20] recently predicted, using a heuristic assumption, that class numbers of real abelian fields of prime conductor are most likely very small compared to known upper bounds.

In his work Schoof also presented and applied an efficient method to compute class number divisors in the case of prime conductors. Koyama and Yoshino [11] presented another approach that allows practical computation. The methods also apply to prime power conductors, but for composite conductors (i.e. conductors having different prime divisors) the Galois module structure of (Hasse's) cyclotomic units is more complicated, due to the fact that different subfields may have different conductors, and thus generalizing the method in this direction is more difficult.

Our approach is to study previously known results that allow computations for composite conductors and to combine them with some ideas from the works mentioned above. We present a method to compute class number divisors for any real abelian field and produce a table of such divisors. By heuristic assumptions similar to Schoof's we predict it to contain all odd prime divisors not dividing the degree of the field in question.

H.-W. Leopoldt in his article [13] generalized Kummer's classical results on the divisibility of class numbers to any real abelian field. His main result is that if an odd prime p not dividing the degree of the field is a divisor of the class number, then a certain rational product of generalized Bernoulli numbers is divisible by p. By applying the p-adic class number formula, W. Schwarz [21] was able to give a simple computational criterion equivalent to Leopoldt's criterion, and he computed for all real abelian fields of conductor $f \leq 500$ a table of all primes $p < 100000$ which possibly divide the class number. The table shows that for a fixed conductor there are usually roughly 5 to 20 primes satisfying Leopoldt's condition. But Leopoldt actually proved a somewhat deeper fact to be able to state his result, and this is what we apply to sharpen the results of Schwarz. Our procedure also makes it possible to sieve out the actual class number divisors from Schwarz's table.

We will first discuss the group theoretic background of Leopoldt's method by applying some earlier results of Leopoldt [12]. This will shed more light on the method of Schwarz. Then we present an additional technique to check if the primes found with Schwarz's method actually come from class numbers. We

limit the computation to prime divisors not dividing $2[K : \mathbf{Q}]$, since the primes dividing the degree of the field do not behave similarly and since for the prime 2 there are better techniques available. We mention here however that Schwarz's method could also be used for some primes dividing the degree; indeed, in many cases one could at least prove that a prime dividing the degree does *not* divide the class number.

Acknowledgment

The author wishes to thank Professor Tauno Metsänkylä for his advice and support.

2 Decomposition of class number

Leopoldt in his thesis [12] presented an arithmetic characterization of a real abelian field, continuing work of Hasse. A main idea was to apply the Wedderburn decomposition of the rational (and later p-adic) Galois group ring to the group of units of an abelian field. Leopoldt was able to reduce the study of the class groups of abelian fields with noncyclic Galois group essentially to the cyclic subfields corresponding to the classes of conjugate characters of the field. We review here only the definitions and results necessary for our study.

Let K be a real abelian field of conductor f with Galois group G of order g. Denote by $\widehat{\chi}$ a rational-irreducible character of K, i.e. $\widehat{\chi} = \sum_k \chi^k$, where the sum runs through the $\mathbf{Q}$-conjugacy class $\widetilde{\chi} = \{\chi^k \mid (k, \operatorname{ord} \chi) = 1\}$ of a character χ of K. The values of $\widehat{\chi}$ are in $\mathbf{Z}$. Denote by f_χ, g_χ and $\operatorname{Ker} \chi$ respectively the common conductor, order and kernel of the $\mathbf{Q}$-conjugates of χ. There is a one-to-one correspondence between the $\mathbf{Q}$-conjugacy classes of the character group and the cyclic subfields of K, given by $\widetilde{\chi} \longleftrightarrow \langle\chi\rangle$; denote the cyclic field corresponding to $\widetilde{\chi}$ by K_χ. Its degree is g_χ, its conductor f_χ, and $\operatorname{Gal}(K_\chi/\mathbf{Q}) = G_\chi \simeq G/\operatorname{Ker} \chi \simeq \langle\chi\rangle$.

The group algebra $\mathbf{Q}[G] = \{\sum_{\sigma\in G} a_\sigma \sigma \mid a_\sigma \in \mathbf{Q}\}$ admits the Wedderburn decomposition

$$\mathbf{Q}[G] = \bigoplus_{\widetilde{\chi}} \mathbf{Q}[G]e_{\widetilde{\chi}} \simeq \bigoplus_{\widetilde{\chi}} \mathbf{Q}(\zeta_{g_\chi})$$

via the rational orthogonal idempotents $e_{\widetilde{\chi}} = \frac{1}{g}\sum_{\sigma\in G} \widehat{\chi}(\sigma^{-1})\sigma$. Here and hereafter we use the notation $\zeta_m = e^{2\pi i/m}$ for any $m \in \mathbf{N}$. The maximal order of $\mathbf{Q}[G]$ is $\bigoplus_{\widetilde{\chi}} \mathbf{Z}[G]e_{\widetilde{\chi}} \simeq \bigoplus_{\widetilde{\chi}} \mathbf{Z}[\zeta_{g_\chi}]$ and $\mathbf{Z}[G]$ is of finite index $g \cdot Q_G$ in it as a subgroup, with $Q_G \in \mathbf{Z}$ containing only primes dividing g.

As a $\mathbf{Q}[G]$-module, the unit group E_K of K decomposes similarly in the form $E_K = \bigoplus_{\widetilde{\chi}} E_K^{e_{\widetilde{\chi}}}$. Rather than studying this decomposition directly, one introduces a subgroup E^{K+} of E_K of finite index; see below. Let $N_{K_\chi/k}$ denote the norm

from K_χ to its subfield k, and define in E_{K_χ} the group of χ-relative units

$$E_\chi = \{\varepsilon \in E_{K_\chi} \mid N_{K_\chi/k}(\varepsilon) = \pm 1 \quad \forall\, k \subsetneq K_\chi\}$$

(Leopoldt uses the notation $E^+_{\widetilde{\chi}}$ and the term narrow $\widetilde{\chi}$-relative units). This is a subgroup of the units of K_χ of rank $\varphi(g_\chi)$ (where φ is the Euler function), and it has a subgroup of χ-relative cyclotomic units

$$F_\chi = \langle -1, \eta^\tau \mid \tau \in G_\chi \rangle$$

which is of finite index

$$h_\chi = [E_\chi : F_\chi].$$

The element η is defined as follows: Let H be the subgroup of $(\mathbf{Z}/f_\chi\mathbf{Z})^\times$ corresponding to $\mathrm{Gal}(\mathbf{Q}(\zeta_{f_\chi})/K_\chi)$, and let $H^+ \subset \mathbf{Z}$ be a system of representatives of $H/\{\pm 1\}$. Define

$$\Theta_\chi = \prod_{a \in H^+} (\zeta_{2f_\chi}^a - \zeta_{2f_\chi}^{-a}), \quad \Lambda_\chi = \prod_{\ell \mid g_\chi} (1 - \sigma^{g_\chi/\ell}), \tag{2.1}$$

where ℓ runs through all prime divisors of g_χ and σ is a generator of G_χ; then $\Theta_\chi^{\sigma-1}$ is a unit of K_χ and $\eta = \Theta_\chi^{\Lambda_\chi}$.

Both E_χ and F_χ depend only on $\widetilde{\chi}$ and thus are independent of the choice of K containing K_χ. The groups of absolute values, $|E_\chi| \simeq E_\chi/\{\pm 1\}$ and $|F_\chi| \simeq F_\chi/\{\pm 1\}$, are modules over $\mathbf{Z}[G_\chi]e_{\widetilde{\chi}} \simeq \mathbf{Z}[\zeta_{g_\chi}]$. Another characterization of the χ-relative units is that they are the units $\varepsilon \in E_{K_\chi}$ satisfying $|\varepsilon|^{e_{\widetilde{\chi}}} = |\varepsilon|$; in particular $|\varepsilon| \in E_K^{e_{\widetilde{\chi}}}$.

When considering E_χ as a subgroup of the units of K we see that the direct product $E^{K+} = \mathrm{dir}\prod_{\widetilde{\chi}} |E_\chi|$ over all the rational characters of K forms a group of units of finite index, say Q_K^+, in the group E_K. Using this decomposition of the unit group and a similar decomposition of the regulator of K, we may split the class number of K in the form (see [12, p. 41])

$$h_K = \frac{Q_K^+}{Q_G} \prod_{\widetilde{\chi}} h_\chi,$$

where Q_K^+ and Q_G are rational integers as explained above, and the product runs through the conjugacy classes $\widetilde{\chi}$ of K. The number Q_K^+ is hard to compute in general. The quotient Q_K^+/Q_G is usually not integral. The numbers Q_K^+ and Q_G comprise only of primes dividing $2g$, and as we assumed that p is not a divisor of $2g$, we may conclude that the p-part of the class number h_K of K is equal to the product of the p-parts of h_χ:

$$h_{K,p} = \prod_{\widetilde{\chi}} h_{\chi,p}.$$

Remark 2.1. Leopoldt also shows that the numbers h_χ are norms of some ideals in $\mathbf{Z}[\zeta_{g_\chi}]$. It follows that once p divides h_χ then also p^{f_p} divides h_χ, where f_p is the residue class degree of p.

For $p \nmid 2g$ we have $g^{-1} \equiv a_k \pmod{p^k}$ for some $a_k \in \mathbf{Z}$ with $k > 0$, and thus we may split the p-class group Cl_p of K as a module over $\mathbf{Z}[G]$ through the idempotents $e_{\widetilde{\chi}}$ (define $\alpha^{1/g} = \alpha^{a_k}$ for $\alpha \in \mathrm{Cl}_p$ of order p^k). We obtain the decomposition (see [12, p. 44])

$$\mathrm{Cl}_p = \mathrm{dir} \prod_{\widetilde{\chi}} \mathrm{Cl}_{\chi,p}, \tag{2.2}$$

where $\#\mathrm{Cl}_{\chi,p} = h_{\chi,p}$. The $\mathbf{Z}[\zeta_{g_\chi}]$-module $\mathrm{Cl}_{\chi,p} = \mathrm{Cl}_p^{e_{\widetilde{\chi}}}$ depends only on K_χ and can be characterized as the group of those ideal classes of order a power of p in K_χ whose relative norm to any subfield $L \subsetneq K_\chi$ is equal to 1 (see [13]). Thus we also gain structural information on the class group by computing the values of all the h_χ.

Leopoldt [13] showed the following fact when proving his theorem about the class number divisibility referred to in the introduction. The proof is based on the decomposition of the p-class group, the reflection theorem and Stickelberger theorem.

Lemma 2.2. *Let p be an odd prime dividing neither the conductor nor the degree of the real abelian field K and let χ be a character of K. If $\mathrm{Cl}_{\chi,p} \neq 1$, then*

$$\prod_{\psi \in \widetilde{\chi}} B_{p-1,\psi} \equiv 0 \pmod{p},$$

where $B_{k,\psi}$ is the kth generalized Bernoulli number associated to ψ.

Note that the above product over the conjugacy class $\widetilde{\chi}$ of χ is rational.

Leopoldt also obtained a result in the ramified case $p \mid f$, $p^2 \nmid f$, but we leave it out from this study for the sake of simplicity; in the practical computations we check the case $p \mid f$ with another method.

Remark 2.3. There exist more recent results on the decomposition of the class group through rational p-adic characters that could allow more precise computations; see for example an article of Aoki [1] on the structure of p-adic parts of the class group. But computations with p-adic numbers may be more difficult or even impossible to perform in practice (cf. [10]). In order to preserve efficiency of our algorithms, we prefer the rational approach. Schoof on the other hand bases his method on Gras's conjecture about the relationship between the p-adic parts of the class groups and of the units modulo cyclotomic units, while all his computations are in rational numbers. Gras's conjecture was proved by R. Greenberg in the case p not dividing the degree; he in fact showed that the orders of the p-adic parts of the class group and units modulo cyclotomic units coincide. This gives a connection between Schoof's method and ours.

3 The algorithm

We first give an outline of the method. As presented in the preceding section, we will omit the prime 2 and the primes dividing the degree g of the field K in question. To check if a prime $p \nmid 2g$ divides the class number of K, it suffices to run the test for all $h_{\chi,p}$ separately, i.e. it is sufficient to study only cyclic fields K_χ and cyclic modules $|F_\chi|$ of cyclotomic units. When computing h_χ we always choose $K = K_\chi$.

The method consists of three parts. First we use Leopoldt's result 2.2 with the method of Schwarz [21], and we are left with a small number of primes that need to be tested further; for all the other primes p the class number is not divisible by p. In view of Leopoldt's result, Schwarz's method not only gives the primes p possibly dividing the class number h_K but also specifies the h_χ that may admit the divisor p.

The second step consists of a search for cyclotomic units that are pth powers in the unit group, extending an idea of van der Linden [14]. In this way we are able to eliminate all the primes not dividing h_χ.

Passing these tests is a necessary condition for $p \mid h_\chi$, and after them we have a strong belief that p could divide the class number factor h_χ, but this is still not a proof. To verify that $p \mid h_\chi$ we finally check whether the pth root of a unit found in the second step has a minimum polynomial $\in \mathbf{Z}[x]$. This follows an idea in an article of G. and M.-N. Gras [8].

Moreover, we provide a method to check whether h_χ is divisible by a higher power of p. This is also based on [8].

We limited the search to the fields of conductor $f \leq 2000$ and to the primes $p < 10000$. In theory there could be larger primes dividing these class numbers, but the heuristics and the results of the computations (the largest prime factor found was 379) show this to be very unlikely.

4 Schwarz's method

We now describe the first step of the computation. Let $K_0 = \mathbf{Q}(\zeta_f + \zeta_f^{-1})$ be the maximal real abelian field of conductor f. As is clear from the preceding discussion, to study the p-divisibility of the class numbers of real abelian fields of conductor f we have to compute the (χ, p)-part $h_{\chi,p}$ of the class number of K_0 for all characters χ of K_0.

Let χ be a character of K_0. Since h_χ is independent of the choice of the field containing K_χ, we may always assume f to be chosen minimal, i.e. $f = f_\chi$. In the first step we also assume $p \nmid f$; the primes dividing f will be checked in the second step of the algorithm. We choose a bound for primes $p \nmid 2 f g_\chi$ to test.

Denote by $[a]$ the integer part of $a > 0$. We begin with a lemma, which was proved by Schwarz [21, pp. 45–46].

Lemma 4.1. *If χ has conductor f and order n, then*

$$B_{p-1,\chi} \equiv -\chi(p) \sum_{i=1}^{f-1} \chi(i) \sum_{\nu=1}^{[\frac{pi}{f}]} \nu^{-1} f^{-1} \pmod{\mathcal{P}_\chi} \tag{4.1}$$

for a prime ideal $\mathcal{P}_\chi \mid p$ in $\mathbf{Z}[\zeta_n]$.

Proof. We sketch a proof. Fix an embedding of the field of all algebraic numbers in an algebraic closure $\mathbf{\Omega}_p$ of the p-adic field $\mathbf{Q}_p$ and regard all algebraic elements as being in $\mathbf{\Omega}_p$. The congruence $\alpha \equiv \beta \pmod{p^n}$ with $\alpha, \beta \in \mathbf{\Omega}_p$ means that the p-exponent of $\alpha - \beta$ is $\geq n$. Write shortly $\zeta_f = \zeta$.

By using properties of p-adic L-functions $L_p(s, \chi)$ we have

$$B_{p-1,\chi} \equiv L_p(2-p, \chi) \equiv L_p(1, \chi) \pmod{p}.$$

Metsänkylä [15] shows that

$$L_p(1, \chi) \equiv -\sum_{i=1}^{f-1} b_i \chi(i) \pmod{p} \tag{4.2}$$

with rational integers b_i mod p defined by

$$\lambda(\zeta) = \frac{(\zeta-1)^p - (\zeta^p - 1)}{p(\zeta^p - 1)} \equiv \sum_{i=1}^{f-1} b_i \zeta^i \pmod{p}.$$

(By Schwarz, p.43, the number $\lambda(\zeta)$ mod p equals the Fermat quotient of $\zeta^p - 1$.)

Let $a \in \mathbf{Z}$, $a \equiv p^{-1} \pmod{f}$. Since $\frac{1}{p}\binom{p}{k} \equiv \frac{1}{k} \pmod{p}$ we may write

$$(1-\zeta)\lambda(\zeta^a) \equiv \sum_{\mu=0}^{f-1} c_\mu \zeta^\mu \pmod{p}$$

with

$$c_\mu \equiv \sum_{\substack{k=1 \\ ak \equiv \mu \pmod{f}}}^{p-1} k^{-1} \equiv \sum_{\nu=[\frac{p(\mu-1)}{f}]+1}^{[\frac{p\mu}{f}]} \nu^{-1} f^{-1} \pmod{p}.$$

Define the numbers b_i for all $i \in \mathbf{Z} \backslash f\mathbf{Z}$ by periodicity mod f. We have

$$(1-\zeta)\lambda(\zeta^a) \equiv (1-\zeta) \sum_{i=1}^{f-1} b_{pi} \zeta^i \equiv \sum_{i=1}^{f-1} (b_{pi} - b_{p(i-1)}) \zeta^i \pmod{p}.$$

Consequently,

$$b_{pi} \equiv \sum_{\nu=1}^{[\frac{pi}{f}]} \nu^{-1} f^{-1} \pmod{p}.$$

By the formula (4.2),

$$L_p(1,\chi) \equiv -\sum_{i=1}^{f-1} b_{pi}\chi(pi) \pmod{p}.$$

We conclude that the congruence (4.1) holds mod p (in $\mathbf{\Omega}_p$). The claim follows since the numbers in (4.1) are p-integers in the field $\mathbf{Q}(\zeta_n)$. □

Denote by $\Phi_n(x)$ the nth cyclotomic polynomial.

Proposition 4.1. *Let f be the conductor and $n = g_\chi$ the order of χ. Let*

$$\lambda : (\mathbf{Z}/f\mathbf{Z})^\times \to \{0,\dots,n-1\}$$

be defined by $\chi(i) = \zeta_n^{\lambda(i)}$. If the prime $p \nmid 2fn$ divides the h_χ-part of the class number of K_χ, then

$$\mathrm{GCD}_{\mathbf{F}_p[x]}\Big(\sum_{\substack{i=1\\(i,f)=1}}^{f-1} a_i x^{\lambda(i)}, \Phi_n(x)\Big) \neq \overline{1}, \tag{4.3}$$

where $a_i \equiv \sum_{\nu=1}^{[\frac{pi}{f}]} \nu^{-1} f^{-1} \pmod{p}$.

Proof. Assume $p \mid h_\chi$. By Lemma 2.2, $\prod_{\chi\in\widetilde{\chi}} B_{p-1,\chi} \equiv 0 \pmod{p}$. Hence it follows from (4.1) that

$$\prod_{\chi\in\widetilde{\chi}} \sum_{i=1}^{f-1} a_i\chi(i) \equiv 0 \pmod{p}.$$

Since the conjugates χ^σ of χ satisfy $\chi^\sigma(i) = \zeta_n^{k\lambda(i)}$, $(k,n)=1$, and since the zeros of $\Phi_n(x)$ are ζ_n^k, $(k,n)=1$, we have

$$\prod_{\chi\in\widetilde{\chi}} \sum_{\substack{i=1\\(i,f)=1}}^{f-1} a_i\chi(i) = \prod_{\substack{k=1\\(k,n)=1}}^{n-1} \sum_{\substack{i=1\\(i,f)=1}}^{f-1} a_i\zeta_n^{k\lambda(i)} = \mathrm{Res}\big(\Phi_n(x), \sum_{\substack{i=1\\(i,f)=1}}^{f-1} a_i x^{\lambda(i)}\big),$$

where $\mathrm{Res}(\cdot,\cdot)$ is the resultant. Finally, p divides $\mathrm{Res}(f(x),g(x))$ if and only if $\mathrm{GCD}_{\mathbf{F}_p[x]}(f(x),g(x)) \neq \overline{1}$. The claim follows. □

The proof of the proposition is essentially found in Schwarz's thesis. He shows that the computational complexity of the method is $O(p+f_\chi+g_\chi^2)$. Schwarz used the result to produce a table of possible class number divisors for any abelian field of conductor ≤ 500. By resorting to Leopoldt's decomposition of class number the results become more transparent in the case of composite conductor. In particular we know explicitly the factor group of units that is of order h_χ.

Remark 4.2. From the p-adic class number formula one finds that the primes $p \nmid fg_\chi$ satisfying (4.3) but not dividing the class number must satisfy $v_p(R_p(K_\chi)) \geq g_\chi$, where v_p denotes the normalized p-adic valuation and $R_p(K_\chi)$ is the p-adic regulator of the field K_χ (trivially $v_p(R_p(K_\chi)) \geq g_\chi - 1$). In this way we obtain some knowledge of the p-adic regulator without knowing the fundamental units. One could also use the method and the p-adic class number formula in many cases to check whether the class number is not divisible by a prime dividing the degree of the field. With slight changes to the preceding method one could also compute the p-exponent of the (p-adic) product $h_K R_p(K)$, thus obtaining an upper bound for the p-exponent of the class number. We plan to discuss this more precisely in a forthcoming paper.

5 Second step

In [14] van der Linden introduced a method with which he could show by computation that $p \nmid h_K$ in some cases. However, his use of the group of units modulo (Hasse's) cyclotomic units is problematic in general, since one may need to combine unit groups of subfields in order to obtain groups of full rank (see [22, p.150]). We avoid this problem by applying a similar procedure to the groups E_χ/F_χ.

To check if $h_{\chi,p} \neq 1$ we need to analyze the structure of the group E_χ/F_χ. As noted before, $E_\chi/\{\pm 1\}$ and $F_\chi/\{\pm 1\}$ are $\mathbf{Z}[\zeta_{g_\chi}]$-modules. Recalling that $\varepsilon^{e_{\tilde{\chi}}} = \pm\varepsilon$ for any $\varepsilon \in E_\chi$ and $\mathbf{Z}[G_\chi]e_{\tilde{\chi}} \simeq \mathbf{Z}[\zeta_{g_\chi}]$, we may also regard $|E_\chi|$ and $|F_\chi|$ as $\mathbf{Z}[G_\chi]$-modules. Thus F_χ/F_χ^p admits an $\mathbf{F}_p[G_\chi]$-module structure.

It is easy to show that $(E_\chi/F_\chi)_p \simeq (E_\chi^p \cap F_\chi)/F_\chi^p$, where $(E_\chi/F_\chi)_p$ is the p-elementary subgroup (the group of elements of order p). The group $(E_\chi^p \cap F_\chi)/F_\chi^p$ is an $\mathbf{F}_p[G_\chi]$-submodule of F_χ/F_χ^p. If nontrivial, it must contain a minimal submodule of F_χ/F_χ^p. Let this be F_i/F_χ^p; then we have $F_i \subseteq E_\chi^p$. On the other hand, if F_j/F_χ^p is such a minimal submodule of F_χ/F_χ^p that $F_j \subseteq E_\chi^p$, then F_j/F_χ^p is a submodule of $(E_\chi^p \cap F_\chi)/F_\chi^p$. Since the minimal submodules are disjoint, the p-exponent of h_χ is at least the number of minimal submodules F_i/F_χ^p satisfying $F_i \subseteq E_\chi^p$.

In order to prove that $h_{\chi,p} = 1$ it suffices to compute all the minimal submodules of F_χ/F_χ^p and to check that all of them contain elements that are not pth powers of units. This is not difficult, as the minimal submodules are cyclic and easily determined by the following proposition and remark. Recall that the $\mathbf{Z}[G_\chi]$-module $|F_\chi|$ is generated by $\eta = \Theta_\chi^{\Lambda_\chi}$, where Θ_χ and Λ_χ are defined by (2.1).

Proposition 5.1. *Assume that* $p \equiv 1 \pmod{g_\chi}$. *The minimal* $\mathbf{F}_p[G_\chi]$*-submodules of* F_χ/F_χ^p *are* $\langle \eta^{\Phi_{g_\chi}(\sigma)/(\sigma - i)} \rangle F_\chi^p$, *where* i *runs through all the zeros of* $\Phi_{g_\chi}(x) \pmod{p}$ *and* σ *is a generator of* G_χ.

Proof. Consider the $\mathbf{F}_p[G_\chi]$-homomorphism

$$\tau : \mathbf{F}_p[G_\chi] \to F_\chi/F_\chi^p, \quad \delta \mapsto \eta^\delta F_\chi^p.$$

It is obviously well-defined and surjective. Its kernel is an $\mathbf{F}_p[G_\chi]$-module, i.e. an ideal in the principal ideal ring $\mathbf{F}_p[G_\chi] \simeq \mathbf{F}_p[x]/\langle x^{g_\chi} - 1\rangle$. Since F_χ is of finite index in E_χ, the $\mathbf{Z}$-rank of F_χ is equal to $\varphi(g_\chi)$, thus the $\mathbf{F}_p$-rank of F_χ/F_χ^p is $\varphi(g_\chi)$.

Trivially $\Theta_\chi^{\sigma^{g_\chi}-1} = \pm 1$. Write $\sigma^{g_\chi} - 1 = \prod_{d|g_\chi} \Phi_d(\sigma)$. Since Λ_χ is divisible by all the $\Phi_d(\sigma)$ with $d \neq g_\chi$, we have $\eta^{\Phi_{g_\chi}(\sigma)} = \pm 1$. Consequently, the kernel $\mathrm{Ker}(\tau) = \langle \Phi_{g_\chi}(\sigma)\rangle$.

By the assumption on p, the cyclotomic polynomial $\Phi_{g_\chi}(x)$ factors completely $(\mathrm{mod}\ p)$ and we have the evident $\mathbf{F}_p[G_\chi]$-isomorphisms

$$\mathbf{F}_p[G_\chi]/\langle \Phi_{g_\chi}(\sigma)\rangle \simeq \mathbf{F}_p[x]/\langle x^{g_\chi} - 1, \Phi_{g_\chi}(x)\rangle \simeq \mathbf{F}_p[x]/\langle \Phi_{g_\chi}(x)\rangle \simeq (\mathbf{F}_p)^{\varphi(g_\chi)}.$$

The minimal submodules of $(\mathbf{F}_p)^{\varphi(g_\chi)}$ are $\langle (1,0,\ldots,0)\rangle, \ldots, \langle (0,\ldots,0,1)\rangle$. By the above isomorphism, they correspond to $\langle \Phi_{g_\chi}(\sigma)/(\sigma - i)\rangle$ in $\mathbf{F}_p[G_\chi]/\langle \Phi_{g_\chi}(\sigma)\rangle$, where $\sigma - i$ runs through the factors of $\Phi_{g_\chi}(\sigma)\ (\mathrm{mod}\ p)$. The claim follows. □

Remark 5.1. The proposition generalizes to all primes not dividing g_χ. Choose the smallest $f_p \geq 1$ such that $p^{f_p} \equiv 1\ (\mathrm{mod}\ g_\chi)$. The g_χth cyclotomic polynomial factors over $\mathbf{F}_p$ into $\varphi(g_\chi)/f_p$ different polynomials $f_i(x)$ of degree f_p, hence $\mathbf{F}_p[G_\chi]/\langle \Phi_{g_\chi}(\sigma)\rangle \simeq \mathrm{GF}(p^{f_p})^{\varphi(g_\chi)/f_p}$. Then the minimal submodules of F_χ/F_χ^p are $\langle \eta^{\Phi_{g_\chi}(\sigma)/f_i(\sigma)}\rangle$.

Note that if a prime p of order f_p mod g_χ divides h_χ, then also p^{f_p} divides h_χ. This follows from Remark 2.1.

To examine if $F_i \subseteq E_\chi^p$ it thus suffices to check whether $\eta^{\Phi_{g_\chi}(\sigma)/f_i(\sigma)}$ is the pth power of some $\varepsilon \in E_\chi$. We explain how this will be done. Later we will also need the fact that $\varepsilon \notin F_\chi$; this follows from the nontriviality of F_i/F_χ^p.

Choose a prime $q \equiv 1\ (\mathrm{mod}\ 2p\, f_\chi)$ and some $b \in \mathbf{Z}$ satisfying the conditions $b^{2f_\chi} \equiv 1\ (\mathrm{mod}\ q)$, $b \not\equiv 1\ (\mathrm{mod}\ q)$. Then $\zeta_{2f_\chi} \equiv b\ (\mathrm{mod}\ \mathcal{Q})$ for some prime ideal $\mathcal{Q}$ above q in $\mathbf{Q}(\zeta_{2f_\chi})$. By writing $\eta^{\Phi_{g_\chi}(\sigma)/f_i(\sigma)}$ as a rational function $r(\zeta_{2f_\chi})$, we examine whether

$$r(b)^{\frac{q-1}{p}} \equiv 1 \pmod{q}. \tag{5.1}$$

If this congruence holds, we choose another pair (q, b) and repeat the test. If the congruence does not hold for some pair, we conclude that $F_i \not\subseteq E_\chi^p$. If for every submodule F_i there exists such a pair (q, b) not satisfying the congruence, we have the result $p \nmid h_\chi$. Otherwise, if there is a prime p and a submodule F_i which pass the congruence test for many pairs, this gives strong evidence that p would divide the class number. But this is not sure, so we still have to apply another method.

Remark 5.2. Instead of ζ_{2f_χ}, we may actually use f_χth roots of 1 in the computations of the second step. In fact, it is an easy exercise to see that $\Theta_\chi^{\sigma-1}$ may always be written as a rational function of ζ_{f_χ}.

6 Third Step

For some $\alpha = \eta^{\Phi_{g_\chi}(\sigma)/f_i(\sigma)}$ satisfying (5.1) for many pairs (q, b), we want to verify that α is a pth power. This is equivalent to showing that $\sqrt[p]{\alpha}$ is an element of K_χ. As a unit of K_χ the element α has g_χ conjugates in K_χ which we all compute. We calculate an approximation of α and its conjugates α^σ as real numbers by noting that

$$\frac{\zeta_{2f}^a - \zeta_{2f}^{-a}}{\zeta_{2f} - \zeta_{2f}^{-1}} = \frac{\sin(a\pi/f)}{\sin(\pi/f)}.$$

If the polynomial $m_p(x) = \prod_\sigma (x - \sqrt[p]{\alpha^\sigma})$ has integral coefficients, then α is a pth power; this is the minimum polynomial of $\sqrt[p]{\alpha}$. Then also $\sqrt[p]{\alpha^\sigma} = \sqrt[p]{\alpha}^{\,\sigma}$ and $\sqrt[p]{\alpha} \in K_\chi$. But since we have used only approximations, this is still not a proof.

Denote by $\widetilde{m}_p$ the polynomial we have computed in this way to approximate m_p. If some coefficient of $\widetilde{m}_p$ is not close to an integer, this shows that α is not a pth power, given that the precision in the computations is adequate. Otherwise, if all the coefficients of $\widetilde{m}_p$ are very close to integers, we round off the coefficients to obtain the supposed minimum polynomial $m_p(x) \in \mathbf{Z}[x]$. We then check whether $m_p(x) \mid m(x^p)$, where $m(x)$ is the minimum polynomial of α. If this holds, it finally proves that m_p is the minimum polynomial of $\sqrt[p]{\alpha}$ and that $\sqrt[p]{\alpha}$ is an element of K_χ.

Since we compute α in F_χ/F_χ^p, note that we may minimize modulo p the absolute values of the coefficients of $\Phi_{g_\chi}(x)/f_i(x) \in \mathbf{Z}[x]$ in order to prevent coefficient explosion.

7 Higher p-powers

Suppose that using the preceding method we have found a prime p with $p \mid h_\chi$. We want to check whether h_χ is divisible by a higher p-power. G. and M.-N. Gras [8] introduced a method with which this verification is in principle possible.

We first give a link between our step 2 and Gras's approach. Using it we are able to check all the cases with $p \equiv 1 \pmod{g_\chi}$ encountered in the computations.

Lemma 7.1. *Assume $p \equiv 1 \pmod{n}$. Let $k \in \mathbf{Z}$ be a zero of $\Phi_n(x)$ modulo p. We have*

$$\frac{\Phi_n(\zeta_n)}{\zeta_n - k} \equiv \pm \frac{N(\zeta_n - k)}{\zeta_n - k} \pmod{p\mathbf{Z}[\zeta_n]},$$

where $N(\gamma)$ denotes the absolute norm of $\gamma \in \mathbf{Z}[\zeta_n]$.

Proof. By the assumption on p, all the zeros of $\Phi_n(x) \pmod{p}$ are of the form k^j, where $(j, n) = 1$. Thus the prime ideals of $\mathbf{Z}[\zeta_n]$ above p are $\mathcal{P}_j = \langle p, \zeta_n - k^j \rangle$,

$(j,n)=1$. Write the claim in the form

$$\prod_{\substack{j=2\\(j,n)=1}}^{n}(\zeta_n-k^j)\equiv\pm\prod_{\substack{j=2\\(j,n)=1}}^{n}(\zeta_n^j-k)\pmod{p\mathbf{Z}[\zeta_n]}.$$

Since $\zeta_n\equiv k\pmod{\mathcal{P}_1}$, this congruence holds mod $\mathcal{P}_1$. Since the automorphisms $\zeta_n\mapsto\zeta_n^j$, $(j,n)=1$, permute the prime ideals, we see that both products contain a factor $\equiv 0\pmod{\mathcal{P}_i}$ for any $i\neq 1$. □

Define $N(\sigma-k)=\prod_{j=2,(j,n)=1}^{n}(\sigma^j-k)$. Assume $p\mid h_\chi$ and $p\equiv 1\pmod{g_\chi}$. By the isomorphism $\mathbf{Z}[\zeta_{g_\chi}]\simeq\mathbf{Z}[G_\chi]/\langle\Phi_{g_\chi}(\sigma)\rangle$ and the lemma we write

$$\frac{\Phi_{g_\chi}(\sigma)}{\sigma-k}\equiv\pm\frac{N(\sigma-k)}{\sigma-k}\pmod{p\mathbf{Z}[\sigma],\Phi_{g_\chi}(\sigma)).}\tag{7.1}$$

Hence the isomorphism induced by τ in the proof of proposition 5.1 implies that $\eta^{\Phi_{g_\chi}(\sigma)/(\sigma-k)}$ is a pth power in E_χ if and only if $\eta^{N(\sigma-k)/(\sigma-k)}$ is a pth power in E_χ. We know that $N(\sigma-k)=pm$ with $p\nmid m$ (if $p\mid m$, change k to some $k+tp$). Thus we have $\eta^{pm/(\sigma-k)}=\varepsilon^p$ for some $\varepsilon\in E_\chi\backslash F_\chi$ (see the paragraph after Remark 5.1). From this it follows that $\varepsilon^{\sigma-k}=\eta^m$.

Let $F_\chi^{'}=\langle -1,\varepsilon^\tau\mid\tau\in G_\chi\rangle$. Then $|F_\chi^{'}|$ is a $\mathbf{Z}[G_\chi]$-module. Since $\varepsilon\notin F_\chi$ but $\varepsilon^p\in F_\chi$ and $\varepsilon^\sigma=\varepsilon^k\eta^m$, we have $[F_\chi F_\chi^{'}:F_\chi]=p$. On the other hand, $p\nmid[F_\chi F_\chi^{'}:F_\chi^{'}]$ since $\eta^m\in F_\chi^{'}$. From $p\mid[F_\chi F_\chi^{'}:F_\chi^m]$ we thus deduce $p\mid[F_\chi^{'}:F_\chi^m]$. Since $[E_\chi:F_\chi^m]<\infty$ we conclude that $[E_\chi:F_\chi^{'}]<\infty$ and that the p-exponent of $[E_\chi:F_\chi^{'}]$ is equal to the p-exponent of h_χ/p.

Now we run the third step using $F_\chi^{'}$ in place of F_χ. Proposition 5.1 holds with ε in place of η. We thus check whether $\varepsilon^{\Phi_{g_\chi}(\sigma)/(\sigma-j)}$ is a pth power for any j satisfying $\Phi_{g_\chi}(j)\equiv 0\pmod p$. By (7.1) this is equivalent to checking whether $\varepsilon^{N(\sigma-j))/(\sigma-j)}$ is a pth power. Using the third step we may compute $\varepsilon=\sqrt[p]{\eta}^{N(\sigma-j)/(\sigma-j)}$ and its conjugates ε^{σ^k} with a sufficient precision. It follows that we may compute an approximation of any conjugate of $\varepsilon^{\Phi_{g_\chi}(\sigma)/(\sigma-j)}$.

In fact one knows a priori the minimal submodules of $F_\chi^{'}/F_\chi^{'p}$ that need to be checked: they correspond to the minimal submodules of F_χ/F_χ^p that were found to contain pth powers. Indeed, assume

$$\varepsilon\in E_\chi\backslash F_\chi,\quad \varepsilon^p=\eta^{N(\sigma-i)/(\sigma-i)};\quad \rho\in E_\chi\backslash F_\chi^{'},\quad \rho^p=\varepsilon^{N(\sigma-j)/(\sigma-j)},$$

where $i\neq j$. Let $\varepsilon_1=\sqrt[p]{\eta}^{N(\sigma-j)/(\sigma-j)}$. If $N(\sigma-i)=p\,m_1$ with $p\nmid m_1$, we have $\eta^{m_1}=\varepsilon^{\sigma-i}$ and so $\varepsilon_1^{m_1}=\rho^{\sigma-i}\in E_\chi$. Since trivially $\varepsilon_1^p\in E_\chi$ and $(p,m_1)=1$, we conclude $\varepsilon_1\in E_\chi$.

This method seems to fail for $p\not\equiv 1\pmod{g_\chi}$. In this case the second step only gives us pth powers explicitly, although we know by the theory that there also exist p^{f_p}th powers, where f_p is the residue class degree. Nevertheless, if we

find in step 2 that $p \mid h_\chi$, we may check whether $\varepsilon = \sqrt[q]{\eta}^{N(f_i(\sigma))/f_i(\sigma)}$ with $q = p^{f_p}$ belongs to $E_\chi \backslash F_\chi$ for some i. In this way we still may find a p^{f_p}th power in E_χ, while it remains unclear whether this is always possible. In computations this was possible in all the cases we confronted. Choose $\langle \varepsilon \rangle = F'_\chi$. A similar reasoning as above shows that the p-exponent of $[E_\chi : F'_\chi]$ is equal to the p-exponent of h_χ / p^{f_p}. Finally, using the second and third steps (with F'_χ in place of F_χ) we can check whether $p \mid (h_\chi / p^{f_p})$.

In this way we were able to verify that among the fields of conductor ≤ 2000 only two h_χ contain p^{f_p} more than once (both with $f_p = 1$). The 17-class number of a 16-degree field of conductor 1921 is 17^3, and the 3-class number of the quadratic field of prime conductor 1129 is 3^2. The latter is also found in Schoof's table [20]. As an extra check we verified that all the other higher p-powers found in his table could be determined with our method.

Remark 7.2. G. and M.-N. Gras [8] used a method similar to our steps 2 and 3 to compute class numbers of small degree fields. They also used Leopoldt's condition similar to step 1 to limit the number of possible divisors. The tables [6], [7] were computed using this method. The aim in [8] was to compute class numbers of real abelian fields using explicit upper bounds that are practical only in small degree fields; hence the efficiency of the algorithm was not as crucial as in our computations. On the other hand the efficiency could be easily improved using the congruence method as in step 2. Gras's method consists of a search of units of $E_\chi^{\mathcal{P}}$ belonging to F_χ , where $\mathcal{P}$ is a prime ideal of $\mathbf{Z}[\zeta_{g_\chi}]$ above p; this amounts to searching for units of the form $(\eta^{N(f_i(\sigma))/f_i(\sigma)})^{1/p^{f_p}}$ with $\mathcal{P} = \langle p, f_i(\zeta_{g_\chi}) \rangle$. This suggests that step 2 could similarly be generalized to search (by the isomorphism $\mathbf{Z}[\zeta_{g_\chi}] \simeq \mathbf{Z}[G_\chi]/\langle \Phi_{g_\chi}(\sigma) \rangle$) for $\mathcal{P}$th powers in E_χ to cover the case of a larger residue class degree.

8 An example of the calculation

We show by an example how the calculations were done. Choose $f = 1261 = 13 \cdot 97$. Let $K_0 = \mathbf{Q}(\zeta_f + \zeta_f^{-1})$. There are 47 real cyclic fields of conductor f corresponding to the nontrivial $\mathbf{Q}$-conjugacy classes of characters of K_0.

We run for any h_χ the first step of the method by checking whether (4.3) holds. All the necessary information for the computation may be gathered from the knowledge of the character χ of K_0. This is the lengthy part of the calculation since we check all the primes $2 < p < 10000$, $p \nmid f$ for all the 47 different h_χ. We find out that there are in total 68 primes (counted with multiplicity) that satisfy (4.3) for some h_χ, of which 10 primes divide g_χ. We continue to the second step only with the primes not dividing g_χ (the 10 discarded primes of course would also contain some information of the class number divisibility, but they would require another method). Usually the number of primes satisfying (4.3) was proportional to the number of real fields of conductor f.

In the second step we check all the remaining 58 cases. We also check for all h_χ the primes 13 and 97 dividing f. There are a total of 152 cases to check. For instance, we have the prime candidate 2689 in the field of degree 96 corresponding to the character $\chi = \chi_{13}^1\chi_{97}^9$ (in an obvious notation). Since $2689 \equiv 1 \pmod{96}$, there are 96 minimal submodules corresponding to various $\alpha_i = \eta^{\Phi_{96}(\sigma)/(\sigma-i)}$. We choose a pair (q, b) and check the congruence (5.1). For instance the pair $(74598239, 46979)$ is appropriate. With this pair the congruence (5.1) is not satisfied for any α_i, thus $2689 \nmid h_\chi$. All the primes are checked similarly; we can handle all the primes not dividing the class number in this way. An example of a prime dividing the class number is given in the following.

Let $p = 97$ and $\chi = \chi_{13}^2\chi_{97}^{10}$. We compute 10 appropriate pairs (q, b) and notice that (5.1) is always satisfied for the minimal submodule corresponding to $f_i(\sigma) = \sigma + 48$ (the specific minimal submodule depends on the choice of the generator σ; we had σ corresponding to $\zeta_f \mapsto \zeta_f^{19}$). We move on to the third step and compute the real approximation of $\eta^{\Phi_{96}(\sigma)/(\sigma+48)}$ and its conjugates. Its minimum polynomial has huge coefficients, thus it is crucial to reduce first the coefficients of $\Phi_{96}(\sigma)/(\sigma + 48) \in \mathbf{F}_{97}[G_\chi]$. Choosing the coefficients with the smallest absolute value mod p seems to be adequate; denote by α the element thus obtained. The precision we needed in this case was over 5000 digits in order to be able to compute the minimum polynomial $m(x)$ of α. The choice of the coefficients of α probably was not ideal. Nevertheless, this was still possible to handle with computer. The minimum polynomial $m_p(x)$ of $\sqrt[p]{\alpha}$ was computed in the same manner; it had much smaller coefficients, the largest with 54 digits. Finally we checked that $m_p(x)$ divides $m(x^p)$. Moreover, we used the method for higher p-powers to verify that $p^2 \nmid h_\chi$.

There were three pairs (p, h_χ) with p not dividing f (indeed, with $p = 5$ or 7) for which we could not find any pairs (b, q) satisfying (5.1). They were all verified with the third step to be actual class number divisors.

All this took about an hour of time with AMD Athlon 2000+ and Mathematica 4.1 [24].

9 Cohen–Lenstra heuristics

Schoof [20] showed, based on a speculative extension of the Cohen–Lenstra heuristics [3], that the class numbers of real abelian fields of prime conductor most likely are relatively small. The same holds for prime power conductors; see Buhler et al. [2]. We see from Section 2 how to treat class groups of fields of any conductor. It would be natural to assume that the predictions given by Schoof on the size of the class groups hold in our case as well. We will show that this is indeed the case.

Cohen and Lenstra give conjectural heuristic assumptions on the properties of finite modules over direct products of Dedekind domains. In particular the as-

sumptions apply to modules over the (unique) maximal order of the group ring $\mathbf{Q}[G]/\sum_{\sigma\in G}\sigma$ with G abelian. Their examples include probabilities for properties of class groups of quadratic fields and real abelian fields, where the p-parts with p dividing the degree had to be excluded; the heuristics were later generalized in [4] to a wider class of fields, and recently Wittmann [23] gave analogous heuristics in some special cases for primes dividing the degree.

To apply the heuristics, one should originally have a large collection of fields of varying conductor and fixed degree. Since our computations are limited to fields of conductor ≤ 2000 and of varying degree, the situation is different, but as was mentioned in [2] and [20], the heuristics and the computed results *together* support the conjecture that the real class groups are usually very small.

We assume for the rest of the section that $p \nmid \#G$. The decomposition (2.2) allows us to define the p-class groups as modules over $\bigoplus_{\widetilde{\chi}\neq\widetilde{1}}\mathbf{Z}[\zeta_{g_\chi}]$; as $\mathrm{Cl}_{1,p}=1$ for the trivial character $1=\chi_0$, we may drop the corresponding part from the direct sum. Then the sum is isomorphic to the maximal order of the group ring $\mathbf{Q}[G]/\sum_{\sigma\in G}\sigma = \mathbf{Q}[G]/e_1\mathbf{Q}[G]$, so that the heuristics may be applied in our case.

For a finite module A over a Dedekind domain R, there is a decomposition $A=\bigoplus_{\mathcal{P}}A_{\mathcal{P}}$, where $\mathcal{P}$ is a prime ideal of R and the $\mathcal{P}$-part $A_{\mathcal{P}}=\{a\in A \mid \mathrm{Ann}_R a \text{ is a power of } \mathcal{P}\}$. Only finitely many $A_{\mathcal{P}}\neq 0$. Now by [3, Example 5.10], assuming heuristics, the probability that $A_{\mathcal{P}}=0$ is equal to $\prod_{k=2}^{\infty}(1-N\mathcal{P}^{-k})$, where the norm $N\mathcal{P}=\#(A/\mathcal{P})$, and the probabilities for different $\mathcal{P}$ are independent.

Let us show how to apply the above probability in our case. Note first that the prime ideals of $\bigoplus_{\widetilde{\chi}\neq\widetilde{1}}\mathbf{Z}[\zeta_{g_\chi}]$ are of the form $\bigoplus_{\widetilde{\chi}\neq\widetilde{1},\widetilde{\psi}}\mathbf{Z}[\zeta_{g_\chi}]\oplus\mathcal{P}$ where $\mathcal{P}$ runs through the prime ideals of $\mathbf{Z}[\zeta_{g_\psi}]$. Their norms are equal to the norms of $\mathcal{P}$. There are $\varphi(g_\chi)/f_p$ prime ideals of $\mathbf{Z}[\zeta_{g_\chi}]$ above any unramified prime p and their common norm is p^{f_p}, where f_p is the order of p mod g_χ. The number of different $\mathbf{Z}[\zeta_{g_\chi}]$ in the decomposition of the rational group ring of a real cyclotomic field is given by the number of $\mathbf{Q}$-conjugacy classes, thus they may be calculated by some computer algebra program or for instance by the following description by Perlis and Walker [19] of rational abelian group algebras: If G is a finite abelian group of order g, we have $\mathbf{Q}[G]\simeq\bigoplus_{d|g}\frac{n_d}{\varphi(d)}\mathbf{Q}(\zeta_d)$, where n_d is the number of elements of order d in G.

The probability that the class group is trivial is therefore

$$P(\mathrm{Cl}=1)=\prod_{\widetilde{\chi}}\prod_{p\in\mathbf{P}}\prod_{\mathcal{P}|p}P(\mathrm{Cl}_{\chi,\mathcal{P}}=1)=\prod_{\widetilde{\chi}}\prod_{p\in\mathbf{P}}\Big(\prod_{k\geq 2}(1-p^{-kf_p})\Big)^{\varphi(g_\chi)/f_p},$$

where $\mathbf{P}$ denotes the set of all prime numbers. Having computed all the p-parts of the class groups for $2<p<10000$, we assume $p>10000$. Then by taking the logarithm and using the estimates

$$-\ln\left(1-\frac{1}{p^{kf_p}}\right)<\frac{1+10^{-8}}{p^{kf_p}}\quad(k\geq 2),\sum_{k\geq 2}p^{-kf_p}=\frac{1}{p^{f_p}(p^{f_p}-1)}\leq\frac{1+10^{-4}}{p^{2f_p}}$$

we obtain

$$-\ln\bigl(P(\mathrm{Cl}_{\chi,p} = 1\,\forall\, p > 10^4)\bigr) < 1.00011\varphi(g_\chi)\sum_{p>10^4}\frac{1}{f_p p^{2f_p}}.$$

The series is dominated by terms with $f_p = 1$, i.e. $p \equiv 1 \pmod{g_\chi}$; the rest is smaller than $\sum_{p>10^4} p^{-4} < 10^{-13}$ (computed via the "prime zeta function" (9.1)). By the prime number theorem for arithmetic progressions, the number of primes $p < n$ with $p \equiv 1 \pmod{g_\chi}$ equals approximately $\#\{p \in \mathbf{P} \mid p < n\}/\varphi(g_\chi)$ for large n. Thus with many different g_χ we have, at least on average,

$$\sum_{p>10^4}\frac{1}{f_p p^{2f_p}} < 10^{-13} + \sum_{\substack{p>10^4\\ p\equiv 1 \pmod{g_\chi}}} p^{-2} \approx \frac{1}{\varphi(g_\chi)}\sum_{p>10^4} p^{-2}.$$

The series over primes may be approximated from its expression in terms of values $\zeta(m)$ of the Riemann zeta function, $m \geq 2$. Indeed, we have

$$\sum_{p\in\mathbf{P}}\frac{1}{p^m} = \sum_{k=1}^{\infty}\frac{\mu(k)}{k}\ln\zeta(km) \tag{9.1}$$

as the Möbius inversion of the logarithm of the Euler product for $\zeta(m)$ (see, e.g. [5]). This gives $\sum_{p\in\mathbf{P}} p^{-2} \approx 0.452247$. Consequently, $\sum_{p<10^4} p^{-2} \approx 0.452238$. It follows that

$$P(\mathrm{Cl}_{\chi,p} = 1\,\forall\, p > 10^4) \approx 0.999990.$$

It is interesting to note that this estimate does not depend on g_χ.

We computed all the (χ, p)-parts of the class groups for $p < 10000$, $f \leq 2000$. For $f \leq 500$ we went up to the bound $p < 100000$ utilizing Schwarz's tables [21] of the first step. For any fixed p, there are a total of 9339 different $\mathbf{Z}[\zeta_{g_\chi}]$-modules $\mathrm{Cl}_{\chi,p}$ for $500 < f \leq 2000$ (1679 when $f \leq 500$), and when substituting this information in the above formulas one obtains from the heuristics that the predicted number of occurrences of nontrivial class group parts $\mathrm{Cl}_{\chi,p}$ for fields of conductor ≤ 2000 would be approximately 443, and that the class number would not contain larger primes for $500 < f \leq 2000$ with probability $\approx 91\%$ (for $f \leq 500$ with $\approx 99\%$). We might exclude from the calculation all class group parts corresponding to fields of small degree since there exist extensive tables for them; then the above probability for $500 < f \leq 2000$ rises to at least 93%. Given that all the computations have produced only small prime divisors compared to the degree of the field, we find it reasonable to believe that the found class number divisors in fact are all the primes dividing h_χ for any $f \leq 2000$, excluding the prime 2 and the primes dividing the degree of the field.

We found 231 nontrivial χ-parts of class groups, which is smaller than the expected number 443, but is still of the same order of magnitude. This supports the belief that the heuristics slightly overestimate the chance of a nontrivial class group for conductors $f \leq 2000$.

10 Tables

In the enclosed tables we present all the prime divisors < 10000 of the class numbers of the real abelian fields of composite conductor $500 < f \leq 2000$ and prime divisors < 100000 for $f \leq 500$, excluding the prime 2 and the primes dividing the degree of the field. The first column indicates the conductor. A character defining the field K_χ is written in the second column. We use the notation χ_{ℓ^ν} for the generating character $\bmod \ell^\nu$ with ℓ a prime > 2. We have $\omega_4(\pm 1 \bmod 4) = \pm 1$ and for $\nu \geq 3$, $\chi_{2^\nu}(5 \bmod 2^\nu) = \zeta_{2^{\nu-2}}$ and $\chi_{2^\nu}(-1 \bmod 2^\nu) = 1$. The representatives of the conjugacy classes of characters were chosen as in [21].

The third column gives the degree $g_\chi = n$ of K_χ and the last column shows the prime divisor p of the class number h_χ; we did not encounter any h_χ having several different prime divisors. The possible exponent of p is the residue class degree of p mod n except for one case. This is a field of conductor 1921, for which we in step 2 found two different submodules containing 17th powers. The search for higher p-powers showed that the class number is divisible by 17^3. We computed with PARI [18] that the 17-class group is of type $\mathbf{Z}/17^2\mathbf{Z} \times \mathbf{Z}/17\mathbf{Z}$.

For any real field K of conductor f, one may read the p-part of class number for any $p < 10000, p \nmid 2[K : \mathbf{Q}]$ by combining the entries of the table (together with Schoof's table of the fields of prime conductor in [20]) for all cyclic subfields K_χ of K of conductor $f_\chi \mid f$. The p-class structure is given by (2.2).

For example, take the field $K = \mathbf{Q}(\zeta_f + \zeta_f^{-1})$ with $f = 1304 = 8 \cdot 163$. Our table gives for h_K twice the prime factor 19, coming from fields with conductor f and $f/2 = 652$ (both of degree 18). By (2.2), the 19-class group is of type $\mathbf{Z}/19\mathbf{Z} \times \mathbf{Z}/19\mathbf{Z}$. In addition, there is a prime factor 3 coming from a quadratic subfield with conductor f. Since 3 divides the degree 324 of K, the 3-class group of K remains unknown; in fact, it could be possible that $3 \nmid h_K$. The class number of $\mathbf{Q}(\zeta_{163} + \zeta_{163}^{-1})$ is 4 (cf. [14]), thus we find that the possible other odd prime factors of h_K must be > 10000.

The results were checked to agree with the tables of real cyclic fields of degree ≤ 6 (cf. [17], [6], [7], [9], [16]). All the class number divisors of fields of degree ≤ 20 were confirmed with PARI. The results in the case of a prime conductor (omitted from the tables) were found to agree with the tables of Schoof [20] and Koyama and Yoshino [11].

f	χ	n	p
212	$\omega_4^1\chi_{53}^{13}$	4	5
316	$\omega_4^1\chi_{79}^{39}$	2	3
321	$\chi_3^1\chi_{107}^{53}$	2	3
427	$\chi_7^3\chi_{61}^{15}$	4	5
469	$\chi_7^3\chi_{67}^{33}$	2	3
473	$\chi_{11}^5\chi_{43}^{21}$	2	3
481	$\chi_{13}^2\chi_{37}^4$	18	19
551	$\chi_{19}^9\chi_{29}^7$	4	5
556	$\omega_4^1\chi_{139}^{23}$	6	7
568	$\chi_8^1\chi_{71}^{14}$	10	11
	$\omega_4^1\chi_8^1\chi_{71}^{35}$	2	3
629	$\chi_{17}^8\chi_{37}^2$	18	19
	$\chi_{17}^4\chi_{37}^{18}$	4	5
651	$\chi_3^1\chi_7^3\chi_{31}^6$	10	11
652	$\omega_4^1\chi_{163}^9$	18	19
676	$\omega_4^1\chi_{169}^3$	52	53
692	$\omega_4^1\chi_{173}^{43}$	4	5
697	$\chi_{17}^8\chi_{41}^{20}$	2	3
703	$\chi_{19}^9\chi_{37}^1$	36	37
	$\chi_{19}^3\chi_{37}^9$	12	13
728	$\chi_8^1\chi_7^3\chi_{13}^3$	4	5
753	$\chi_3^1\chi_{251}^{25}$	10	11
756	$\omega_4^1\chi_{27}^2\chi_7^1$	18	19
763	$\chi_7^3\chi_{109}^9$	12	13
779	$\chi_{19}^9\chi_{41}^1$	40	41
785	$\chi_5^2\chi_{157}^{78}$	2	3
793	$\chi_{13}^1\chi_{61}^{55}$	12	37
808	$\omega_4^1\chi_8^1\chi_{101}^{25}$	4	5
817	$\chi_{19}^9\chi_{43}^{21}$	2	5
819	$\chi_9^1\chi_7^1\chi_{13}^2$	6	7
832	$\omega_4^1\chi_{64}^1\chi_{13}^3$	16	7^2
869	$\chi_{11}^5\chi_{79}^1$	78	79
889	$\chi_7^3\chi_{127}^{21}$	6	7
892	$\omega_4^1\chi_{223}^{111}$	2	3
916	$\omega_4^1\chi_{229}^{57}$	4	5
923	$\chi_{13}^3\chi_{71}^7$	20	61
928	$\omega_4^1\chi_{32}^1\chi_{29}^7$	8	17
935	$\chi_5^1\chi_{11}^5\chi_{17}^4$	4	5
940	$\omega_4^1\chi_5^2\chi_{47}^{23}$	2	3
944	$\omega_4^1\chi_{16}^1\chi_{59}^{29}$	4	5
976	$\omega_4^1\chi_{16}^1\chi_{61}^{15}$	4	5
980	$\omega_4^1\chi_5^1\chi_{49}^6$	28	29
985	$\chi_5^2\chi_{197}^{98}$	2	3
988	$\omega_4^1\chi_{13}^2\chi_{19}^3$	6	7
993	$\chi_3^1\chi_{331}^{165}$	2	3
999	$\chi_{27}^2\chi_{37}^{16}$	9	37

f	χ	n	p
1016	$\omega_4^1\chi_8^1\chi_{127}^{63}$	2	3
1025	$\chi_{25}^1\chi_{41}^7$	40	41
1036	$\omega_4^1\chi_7^2\chi_{37}^5$	36	73
1048	$\chi_8^1\chi_{131}^{26}$	10	11
1080	$\chi_8^1\chi_{27}^1\chi_5^1$	36	37
1101	$\chi_3^1\chi_{367}^{183}$	2	3
1105	$\chi_5^1\chi_{13}^9\chi_{17}^8$	4	5
1113	$\chi_3^1\chi_7^2\chi_{53}^{13}$	12	13
1116	$\omega_4^1\chi_9^2\chi_{31}^{25}$	6	7
1132	$\omega_4^1\chi_{283}^{47}$	6	7
1139	$\chi_{17}^2\chi_{67}^6$	88	89
1141	$\chi_7^2\chi_{163}^{36}$	9	19
1159	$\chi_{19}^2\chi_{61}^{10}$	18	73
1172	$\omega_4^1\chi_{293}^{73}$	4	13
1197	$\chi_9^2\chi_7^5\chi_{19}^{15}$	6	7
1207	$\chi_{17}^1\chi_{71}^{35}$	16	17
1211	$\chi_7^2\chi_{173}^{86}$	6	7
1235	$\chi_5^1\chi_{13}^4\chi_{19}^{15}$	12	13
	$\chi_5^2\chi_{13}^3\chi_{19}^9$	4	5
1241	$\chi_{17}^4\chi_{73}^{18}$	4	5
1243	$\chi_{11}^2\chi_{113}^{14}$	40	41
1257	$\chi_3^1\chi_{419}^{209}$	2	3
1261	$\chi_{13}^2\chi_{97}^{10}$	48	97
	$\chi_{13}^2\chi_{97}^{64}$	6	7
	$\chi_{13}^6\chi_{97}^{24}$	4	5
	$\chi_{13}^4\chi_{97}^{64}$	3	7
1271	$\chi_{31}^2\chi_{41}^{24}$	15	31
	$\chi_{31}^{10}\chi_{41}^{20}$	6	7
	$\chi_{31}^6\chi_{41}^{24}$	5	11
1287	$\chi_9^1\chi_{11}^2\chi_{13}^3$	60	61
1295	$\chi_5^2\chi_7^2\chi_{37}^{10}$	18	19
1304	$\chi_8^1\chi_{163}^{18}$	18	19
	$\omega_4^1\chi_8^1\chi_{163}^{81}$	2	3
1308	$\omega_4^1\chi_3^1\chi_{109}^{18}$	6	7
1311	$\chi_3^1\chi_{19}^2\chi_{23}^{11}$	18	19
1313	$\chi_{13}^6\chi_{101}^{20}$	10	31
1332	$\omega_4^1\chi_9^1\chi_{37}^6$	6	7
1339	$\chi_{13}^3\chi_{103}^{17}$	12	13
1343	$\chi_{17}^1\chi_{79}^{39}$	16	17
1345	$\chi_5^2\chi_{269}^{134}$	2	3
1353	$\chi_3^1\chi_{11}^1\chi_{41}^{12}$	10	11
1355	$\chi_5^2\chi_{271}^{30}$	18	37
1359	$\chi_9^1\chi_{151}^{125}$	6	7
1360	$\omega_4^1\chi_{16}^1\chi_5^1\chi_{17}^{12}$	4	5
1376	$\omega_4^1\chi_{32}^1\chi_{43}^7$	24	5^2
1384	$\chi_8^1\chi_{173}^{86}$	2	3

f	χ	n	p
1385	$\chi_5^2\chi_{277}^{46}$	6	7
	$\chi_5^1\chi_{277}^{207}$	4	5
1387	$\chi_{19}^2\chi_{73}^{18}$	36	17^2
	$\chi_{19}^2\chi_{73}^{22}$	36	37
	$\chi_{19}^2\chi_{73}^{8}$	9	19
1393	$\chi_7^3\chi_{199}^{99}$	2	5
1404	$\omega_4^1\chi_{27}^1\chi_{13}^8$	18	19
1407	$\chi_3^1\chi_7^3\chi_{67}^6$	22	23
1420	$\omega_4^1\chi_5^2\chi_{71}^7$	10	11
1421	$\chi_{49}^3\chi_{29}^{11}$	28	29
1424	$\omega_4^1\chi_{16}^1\chi_{89}^{11}$	8	17
1435	$\chi_5^1\chi_7^1\chi_{41}^{10}$	12	13
1436	$\omega_4^1\chi_{359}^{179}$	2	3
1455	$\chi_3^1\chi_5^1\chi_{97}^6$	16	17
1460	$\omega_4^1\chi_5^1\chi_{73}^{54}$	4	5
1461	$\chi_3^1\chi_{487}^{27}$	18	19
1465	$\chi_5^1\chi_{293}^{219}$	4	3^2
1477	$\chi_7^3\chi_{211}^{21}$	10	11
	$\chi_7^1\chi_{211}^{35}$	6	7
1496	$\omega_4^1\chi_8^1\chi_{11}^1\chi_{17}^8$	10	11
1509	$\chi_3^1\chi_{503}^{251}$	2	3
1513	$\chi_{17}^1\chi_{89}^{11}$	16	17
	$\chi_{17}^8\chi_{89}^{22}$	4	13
1516	$\omega_4^1\chi_{379}^1$	378	379
1525	$\chi_{25}^2\chi_{61}^{24}$	10	11
1547	$\chi_7^1\chi_{13}^1\chi_{17}^{12}$	12	37
1575	$\chi_9^1\chi_{25}^2\chi_7^5$	30	31
1576	$\omega_4^1\chi_8^1\chi_{197}^{49}$	4	3^2
1591	$\chi_{37}^{18}\chi_{43}^2$	42	43
1592	$\omega_4^1\chi_8^1\chi_{199}^{11}$	18	19
	$\omega_4^1\chi_8^1\chi_{199}^{33}$	6	7
1620	$\omega_4^1\chi_{81}^2\chi_5^1$	108	109
1623	$\chi_3^1\chi_{541}^{45}$	12	13
1629	$\chi_9^2\chi_{181}^{18}$	30	31
	$\chi_9^2\chi_{181}^{50}$	18	109
1640	$\omega_4^1\chi_8^1\chi_5^2\chi_{41}^5$	8	3^2
1641	$\chi_3^1\chi_{547}^{273}$	2	5
1643	$\chi_{31}^5\chi_{53}^{13}$	12	13
1651	$\chi_{13}^1\chi_{127}^{63}$	12	5^2
1665	$\chi_9^1\chi_5^1\chi_{37}^{24}$	12	13
1676	$\omega_4^1\chi_{419}^{19}$	22	23
1687	$\chi_7^2\chi_{241}^{80}$	3	13
1688	$\chi_8^1\chi_{211}^{42}$	10	31
1708	$\omega_4^1\chi_7^1\chi_{61}^{50}$	6	7
	$\omega_4^1\chi_7^3\chi_{61}^{30}$	2	3

f	χ	n	p
1729	$\chi_7^2\chi_{13}^3\chi_{19}^3$	12	5^2
	$\chi_7^1\chi_{13}^5\chi_{19}^{12}$	12	13
	$\chi_7^1\chi_{13}^2\chi_{19}^{15}$	6	7
1735	$\chi_5^1\chi_{347}^{173}$	4	5
1736	$\omega_4^1\chi_8^1\chi_7^2\chi_{31}^{15}$	6	7
1739	$\chi_{37}^9\chi_{47}^{23}$	4	5
1749	$\chi_3^1\chi_{11}^5\chi_{53}^2$	26	53
1751	$\chi_{17}^1\chi_{103}^{51}$	16	17
1755	$\chi_{27}^2\chi_5^1\chi_{13}^3$	36	73
1756	$\omega_4^1\chi_{439}^{219}$	2	5
1761	$\chi_3^1\chi_{587}^{293}$	2	7
1765	$\chi_5^2\chi_{353}^{176}$	2	3
1772	$\omega_4^1\chi_{443}^{221}$	2	3
1853	$\chi_{17}^8\chi_{109}^6$	18	19
1855	$\chi_5^2\chi_7^3\chi_{53}^{13}$	4	5
1865	$\chi_5^1\chi_{373}^{93}$	4	5
1872	$\chi_{16}^1\chi_9^2\chi_{13}^{10}$	12	13
1885	$\chi_5^1\chi_{13}^6\chi_{29}^1$	28	29
	$\chi_5^2\chi_{13}^3\chi_{29}^3$	28	113
	$\chi_5^1\chi_{13}^6\chi_{29}^7$	4	5
1887	$\chi_3^1\chi_{17}^4\chi_{37}^{27}$	4	5
1891	$\chi_{31}^3\chi_{61}^{21}$	20	41
	$\chi_{31}^2\chi_{61}^{28}$	15	31
	$\chi_{31}^6\chi_{61}^6$	10	11
1897	$\chi_7^3\chi_{271}^{135}$	2	5
1903	$\chi_{11}^5\chi_{173}^1$	172	173
1904	$\chi_{16}^1\chi_7^3\chi_{17}^3$	16	97
	$\omega_4^1\chi_{16}^1\chi_7^1\chi_{17}^{12}$	12	13
1921	$\chi_{17}^4\chi_{113}^8$	28	29
	$\chi_{17}^1\chi_{113}^{35}$	16	$17\cdot 17^2$
1929	$\chi_3^1\chi_{643}^{321}$	2	3
1935	$\chi_9^2\chi_5^1\chi_{43}^7$	12	13
	$\chi_9^2\chi_5^1\chi_{43}^{21}$	12	13
1937	$\chi_{13}^1\chi_{149}^{111}$	12	109
	$\chi_{13}^6\chi_{149}^{74}$	2	3
1957	$\chi_{19}^9\chi_{103}^{51}$	2	3
1965	$\chi_3^1\chi_5^2\chi_{131}^{13}$	10	11
1971	$\chi_{27}^2\chi_{73}^4$	18	19
1972	$\omega_4^1\chi_{17}^2\chi_{29}^7$	8	3^2
1976	$\chi_8^1\chi_{13}^6\chi_{19}^2$	18	19
	$\chi_8^1\chi_{13}^1\chi_{19}^3$	12	13
1988	$\omega_4^1\chi_7^2\chi_{71}^5$	42	43
	$\omega_4^1\chi_7^1\chi_{71}^{14}$	30	31
1995	$\chi_3^1\chi_5^2\chi_7^2\chi_{19}^3$	6	7
1996	$\omega_4^1\chi_{499}^{249}$	2	5

References

[1] M. Aoki, *Notes on the structure of the ideal class groups of abelian number fields*, Proc. Japan Acad. Ser. A Math. Sci. **81** (2005), no. 5, pp. 69–74.

[2] J. Buhler, C. Pomerance, L. Robertson, *Heuristics for class numbers of prime-power real cyclotomic fields*, High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams, Fields Inst. Commun. **41**, Amer. Math. Soc., Providence, RI (2004), pp. 149–157.

[3] H. Cohen, H. W. Lenstra, *Heuristics on class groups of number fields*, Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), Lecture Notes in Math. **1068**, Springer, Berlin (1984), pp. 33–62.

[4] H. Cohen, J. Martinet, *Étude heuristique des groupes de classes des corps de nombres*, J. Reine Angew. Math. **404** (1990), pp. 39–76.

[5] C.-E. Fröberg, *On the prime zeta function*, BIT **8** (1968), pp. 187–202.

[6] M.-N. Gras, *Méthodes et algorithmes pour le calcul numérique du nombre de classes et des unités des extensions cubiques cycliques de* $\mathbf{Q}$, J. Reine Angew. Math. **277** (1975), pp. 89–116.

[7] M.-N. Gras, *Table numérique du nombre de classes et des unités dans les extensions cycliques réelles de degre* 4 *de* $\mathbf{Q}$, Publ. Math. Fac. Sci. Besançon 1977/78, Fasc. 2, 52 pp.

[8] G. and M.-N. Gras, *Calcul du nombre de classes et des unités des extensions abéliennes réelles de* $\mathbf{Q}$, Bull. Sci. Math. (2) **101** (1977), no. 2, pp. 97–129.

[9] S. Jeannin, *Tables des nombres de classes et unités des corps quintiques cycliques de conducteur* $f \leq 10000$, Publ. Math. Fac. Sci. Besançon 1994/95–1995/96, 40 pp.

[10] S. Kobayashi, *Divisibilité du nombre de classes des corps abéliens réels*, J. Reine Angew. Math. **320** (1980), pp. 142–149.

[11] Y. Koyama and K. Yoshino, *Prime divisors of real class number of* p^r*th cyclotomic field and characteristic polynomials attached to them*, Preprint (2003), 23 pp.

[12] H. W. Leopoldt, *Über Einheitengruppe und Klassenzahl reeller abelscher Zahlkörper*, Abh. Deutsch. Akad. Wiss. Berlin. Kl. Math. Nat. 1953, no. 2 (1954), 48 pp.

[13] H. W. Leopoldt, *Über Klassenzahlprimteiler reeller abelscher Zahlkörper als Primteiler verallgemeinerter Bernoullischer Zahlen*, Abh. Math. Sem. Univ. Hamburg **23** (1959), pp. 36–47.

[14] F. van der Linden, *Class number computations of real abelian number fields*, Math. Comp. **39** (1982), pp. 693–707.

[15] T. Metsänkylä, *An application of the p-adic class number formula*, Manuscripta Math. **93** (1997), pp. 481–498.

[16] S. Mäki, *The determination of units in real cyclic sextic fields*, Lecture Notes in Math. **797**, Springer, Berlin (1980), 198 pp.

[17] B. Oriat, *Groupes des classes d'idéaux des corps quadratiques réels* $\mathbf{Q}(d^{1/2})$, $1 < d < 24572$, Publ. Math. Fac. Sci. Besançon 1986/87–1987/88, Fasc. 2, 65 pp.

[18] PARI/GP, version `2.2.8`, Bordeaux, 2005, `http://pari.math.u-bordeaux.fr/`

[19] S. Perlis and G. Walker, *Abelian group algebras of finite order*, Trans. Amer. Math. Soc. **68** (1950), pp. 420–426.

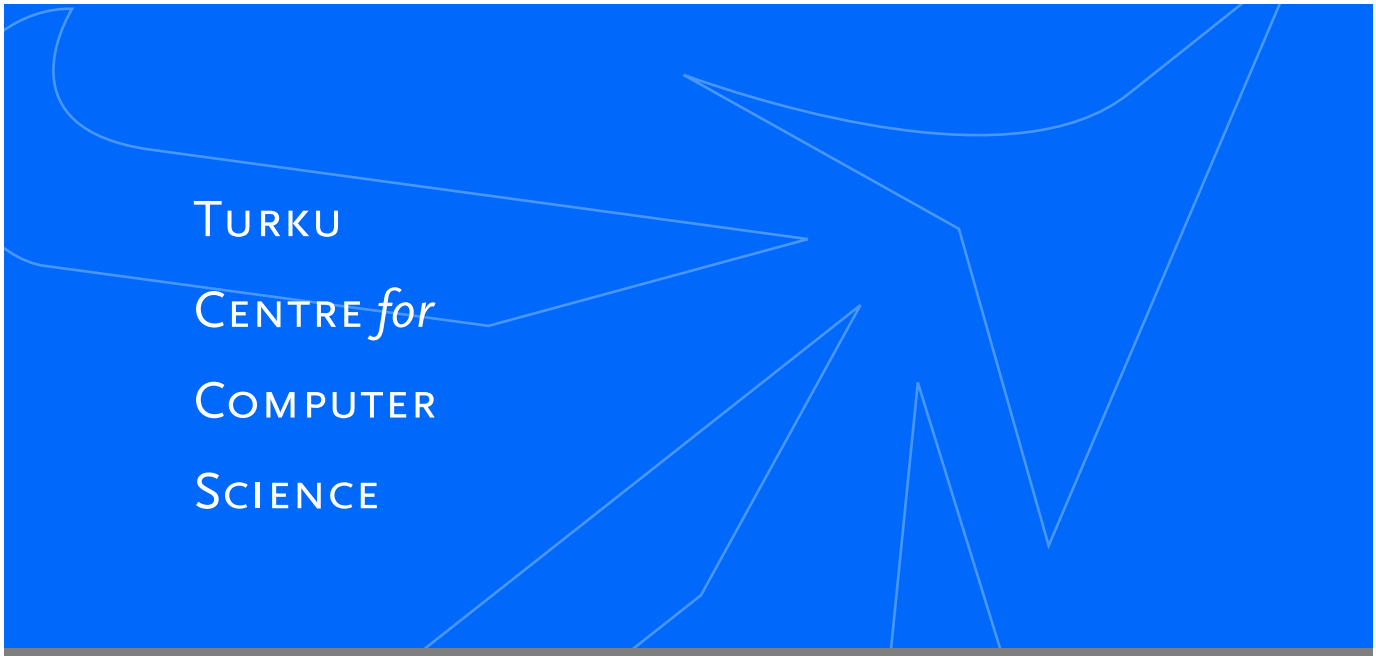
[20] R. Schoof, *Class numbers of real cyclotomic fields of prime conductor*, Math. Comp. **72** (2003), pp. 913–937.

[21] W. Schwarz, *Über die Klassenzahl abelscher Zahlkörper*, PhD Thesis, University of Saarbrücken (1995), 125 pp.

[22] L. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Springer, New York, 1997.

[23] C. Wittmann, *p-class groups of certain extensions of degree p*, Math. Comp. **74** (2005), pp. 937–947.

[24] Wolfram Research, Inc., Mathematica, Version 4.1, Champaign, IL (2001).



Lemminkäisenkatu 14 A, 20520 Turku, Finland | www.tucs.fi

University of Turku
- Department of Information Technology
- Department of Mathematics

Åbo Akademi University
- Department of Computer Science
- Institute for Advanced Management Systems Research

Turku School of Economics and Business Administration
- Institute of Information Systems Sciences

ISBN 952-12-1731-6
ISSN 1239-1891